DLA INTERNET POLICY

1 May 1997

DLA Policy on Disseminating and Obtaining Information Via the Internet and World Wide Web, Intranets and Electronic Mail

This document rescinds CIO-Letter 96-4, dated August 16, 1996.

This document establishes policy, provides procedures and guidance, and assigns responsibilities for the use of the Internet and World Wide Web, Intranets, and electronic mail by military, civilian, and contractor personnel of the Defense Logistics Agency. It applies to all such personnel who use government-furnished resources to disseminate or obtain information via these media.

INDEX

This document is organized into the following sections to make it easy for the user to navigate to the specific information needed:

- **General Policy** provides guidance on **Official Use**, **Non-Official Use**, and **Prohibited Use** of the Internet and on use of the **DLA Intranet** in conducting government business.

- **Review, Release, and Approval Authorities** identifies who must authorize and clear information before it appears on the Internet.

- **Conventions and Etiquette** contains information on **naming** Internet host systems, **e-mail,** **file transfers**, and **Internet chat**.

- **Design Guidelines** describes the recommended structure for homepages, standardized departments, and required linkages.

- **Security** describes the security accreditation required for all Internet and Intranet Web sites.

- **Oversight** describes the recommended make-up of a policy council charged with monitoring DLA Internet and Intranet Web sites to ensure compliance with policy and the appropriateness of content.

- **Government Information Locator Service** describes the procedure for registering the DLA activity's Internet site.

- **Appendix A: Laws and Regulations** references the statutory and regulatory requirements governing information dissemination, storage, and retrieval. Where available, Web site locations for these documents are provided.

- **Appendix B: Definitions** includes terms, acronyms, and abbreviations referenced in this document.

- **Appendix C: Notices** contains suggested warnings and disclaimers.

GENERAL POLICY

The World Wide Web provides the public with user-friendly, graphics-based, multimedia access to information on the Internet. This gives the Defense Logistics Agency and its components a new and powerful means of enhancing DLA's business processes and disseminating publicly releasable information, which can greatly benefit DLA's mission accomplishment. As such, DLA commanders will provide Internet access to all Agency employees and strongly encourage its use as a business and communication tool.

DLA personnel and associated contractors are responsible for ensuring the safe, effective, efficient, and legal use of all government resources. As such, DLA personnel must:

- Exercise the highest standards of professional conduct and responsible behavior with the information they obtain from or make available to the Internet.

- Defend the security of our nation and promote the taxpayers' interests by exercising due caution and protecting information that unscrupulous contractors, foreign governments, or others might use to the disadvantage of the agency, other Department of Defense organizations, or the U.S. government. Examples of what must be protected include proprietary, contractual, operationally sensitive, and classified information.

- Assume that anyone in the world can access the Internet and therefore take all necessary steps to preclude the unauthorized disclosure of information.

DLA Homepage **CIO Homepage** **Internet Policy Index**

OFFICIAL USE

Use of the Internet must be in the interest of the agency and the federal government. Such use should be appropriate in its frequency and duration and related to an employee's assigned duties. For example, the Internet can be used to:

- Obtain or exchange information to support DLA or DoD missions.

- Obtain or exchange information that enhances the professional skills of DLA employees, thereby improving their job performance and benefiting the agency.

- Improve an employee's formal education, when approved by an immediate supervisor.

DLA Homepage **CIO Homepage** **Internet Policy Index**

NON-OFFICIAL USE

In accordance with the March 1996 update of DoD’s Joint Ethics Regulation, DLA personnel are authorized to use government computers to access the Internet for personal purposes if the usage is approved by their commanders and it:

- Does not adversely affect the employee's performance of official duties.

- Serves such legitimate public interests as the following examples:

  - Enhancing employees' professional skills.

  - Educating the employee on the use of the Internet as a business and communication tool.

  - Improving the morale of employees who are stationed away from home for extended periods.

  - Enabling employees’ participation in professional or civic associations.

  - Helping military and civilian personnel to seek job opportunities in the federal government.

Employees should control the frequency and duration of non-official usage to preclude any appearance of impropriety and unnecessary costs to the federal government; in addition, incidental usage should occur on such personal time as breaks, lunch periods, and after-duty hours. Those who do not adhere to this policy will be subject to adverse personnel actions ranging from reprimands to suspension and dismissal.

DLA Homepage **CIO Homepage** **Internet Policy Index**

PROHIBITED USE

It is incumbent upon supervisors to ensure employees are aware that Internet usage can be monitored and leaves a clear audit trail. Examples of prohibited usage that would reflect adversely on DLA include:

- Visiting sites involving pornography.
- Gambling, conducting illegal activities, and soliciting for personal gain.
- Downloading copyrighted software without express permission.
- Downloading without ensuring protection against viruses.
- Misrepresenting personal opinion as official information.
- Engaging in chain letters.

DLA Homepage **CIO Homepage** **Internet Policy Index**

DLA INTRANET

Using the same technology as the Internet, DLA Intranet pages restrict information access to DLA personnel and, in certain instances, selected outsiders─for example, the military services, contractors, and vendors. (While sites that allow access by outside personnel are sometimes referred to as expanded Intranets or Extranets, for purposes of this policy letter, the term Intranet is used.)
In some cases, the only means used to restrict information will be by domain access; e.g., restricted to ".mil" or ".dla.mil" addresses; in other cases involving more sensitive information, outside users must be approved, registered, issued a password or certification card, and notified that their movements on the sites can and will be monitored. **Under no circumstance will classified information be placed on or made accessible by the Internet or unsecured Enterprise-wide Web.**

Examples of unclassified business information that should not be accessible via the unrestricted Internet, but might be made available on an authorized-users-only Intranet, include:

- For Official Use Only information.
- Unclassified information that requires special handling─for example, data intended for limited distribution, and scientific and technical information protected by law.
- Contractor proprietary data and procurement-sensitive information.
- Products with specific licensing or use restrictions.
- Databases and the information therein.

The business and communication advantages of Intranet pages to DLA include:

- Allowing agency personnel worldwide to network better across business areas and to communicate more effectively and speedily.
- Sharing information with a much wider audience than is possible with past technologies.

- Offering outsiders access to product and service information whenever they want it and however they want it from anywhere.

- Reducing costs through different business practices; for example, by publishing policy documents and publications on the Intranet, DLA can dramatically reduce its expenditures on paper, postage, and storage space.

Because information on the DLA Intranet is by definition not available to the public, such information does not require approval by the Public Affairs Office before posting. However, DLA personnel publishing information on these pages must exercise sound business judgment that takes into consideration the do's and don't's mentioned in the sections on **Official Use**, **Non-Official Use**, and **Prohibited Use**.

DLA Homepage **CIO Homepage** **Internet Policy Index**

REVIEW, RELEASE, AND APPROVAL AUTHORITIES

Information placed on the Internet without restricted access is by definition available to anyone in the world. To ensure that such information is not misused—whether inadvertently or deliberately—it is subject to the same legal and regulatory requirements as non-electronic information. These requirements include compliance with the Privacy Act, the Freedom of Information Act, copyright protection, and other **Laws and Regulations**. Accordingly, information must be formally reviewed and approved for release in accordance with DoD Directive 5230.9, "Clearance of DoD Information for Public Release," which is a responsibility assigned to DLA's Public Affairs Officers.

For Internet applications, there will typically be three levels of review, release, and approval authority before information becomes publicly available.

- The **Content Providers** are the functional area experts who must certify that the information proposed for placement on the Internet is unclassified, nonsensitive, nonproprietary, current, accurate, complete, and cleared for public release by appropriate authorities in the business areas and Public Affairs. The Web Server Administrator (or "Webmaster") is responsible for keeping records of such certifications.

- The **Public Affairs Officer**, on behalf of the director or commander, is the release authority for public information. The PAO must ensure that the information has been properly coordinated prior to public release, e.g., with the Office of General Counsel. Reviews must be redone when significant changes are made in the previously released information or a new category of information is added. All DLA activities are encouraged to work with their PAO in developing a coordinated, streamlined review process.

- The **Designated Approval Authority** is the activity's commanding officer, but this authority can be delegated to a representative who in turn is charged with the responsibility of approving and overseeing the activity's Web site. Typically a senior military officer or civilian manager, this individual must ensure the overall appropriateness of the content of Web pages and conduct a network risk analysis as part of a network security plan. This process is essential in determining the appropriate level and placement of security mechanisms to ensure the integrity, authenticity, privacy, and proper availability of a command's information systems and data therein (see the section on **Security** for more information).

In addition, the Chief Information Officer's **Senior Internet Policy Advisor** at DLA headquarters is responsible for ensuring that all DLA Internet applications comply with policy, adhere to statutory and regulatory requirements, and present the agency in a professional and positive manner.

DLA Homepage **CIO Homepage** **Internet Policy Index**

CONVENTIONS AND ETIQUETTE

DLA personnel, all of whom will be given basic Internet access, must comply with the following:

- **Naming Internet Host Systems**. All activities operating DLA-owned servers must follow a naming and addressing convention for host systems that succinctly and clearly identifies the activity and its organizational linkage to DLA. The required convention is: "activity's abbreviation.dla.mil/subordinate links." The address for a homepage of the commander of the contract management site at Northrop Grumman in the Defense Contract Management Command's western district, for example, would be "dcmdw.dla.mil/dcmcng/commander." Exceptions must be approved by the Chief Information Officer.

- **E-mail and File Transfers**.

  - **E-mail**. All DLA personnel must demonstrate ethical behavior in their use of the e-mail capability on the Internet, and they must ensure that the content of their e-mail messages is professional and accurately states agency or Defense Department policies and positions. Personnel should remember that e-mails are considered a public record and should be treated accordingly.

    E-mail must not be used for the indiscriminate dissemination of information that would be more appropriately posted to an electronic bulletin board or to an Intranet electronic conference room (also known as a "chat area"), where users can routinely choose to access and enter into a dialogue with the message sender rather than be forced to read the message.

    Personnel sending e-mail with attachments must be cognizant of technical constraints that can prohibit the receiving party from opening the attachments. Further, users should be wary of opening executable attachments from unfamiliar sources; such attachments can contain not only viruses that will automatically execute but also internal commands that can damage the personal computer. Suspicious attachments should be reported to the systems administrator.

  - **File Transfers**. DLA personnel will not download commercial software or "shareware" that obligates the agency for payment; rather, established acquisition processes must be followed. Users must also ensure that downloaded software is free of viruses and be aware of network disk storage limitations before storing files or data on network resources.

- **Internet Chat**. DLA personnel must use these services judiciously and ensure full compliance with the policies in this document. The Agency address is clearly apparent to others involved in such chats, so those with whom you chat know you are a DLA employee and you must behave accordingly.

DLA Homepage **CIO Homepage** **Internet Policy Index**

DESIGN GUIDELINES

DLA's presence on the Internet consists of the DLA headquarters homepage and homepages for each of the agency's major business areas and their primary-level field activities. To the maximum extent possible, it is recommended that all of these pages have a common look and feel—that is, follow the same format and have common items (described below)—to make it easier for the user to move efficiently from one page to another through a series of interconnected links. Because DLA comprises widely diverse business operations, however, the design of some agency homepages will necessarily vary from the norm in order to provide the most logical arrangement of information.

Standard Navigational Aids. Three standard navigational icons should be located at the end of documents to help the user quickly move about the DLA Web site:

- **DLA Homepage**. This icon returns you to the Agency's homepage.

- **Activity Homepage**. This icon returns you to the homepage of the DLA activity responsible for the document on the screen. This icon and the DLA homepage icon enable users who becomes "lost" in a DLA site to return to "square one."

- **Top of Document**. This icon returns you to the top of the document on your screen.

Common Items. DLA recommends that all agency homepages should include as many of the following common-item links as possible in order to offer the user greater familiarity regarding where to find desired information quickly and easily:

- **Welcome** enables an activity's leader to greet users and provide an overview of the Web site.

- **What's New** contains the latest information about significant initiatives at that activity. This information is typically in the form of a brief synopsis that links to more expansive information elsewhere on the homepage for users who need greater detail.

- **Organization** contains organization charts, a mission and function statement, and a brief history.

- **Buying & Selling** links to contract or requisition information.

- **Initiatives** describes those programs, projects, and activities that DLA is implementing to improve its support of the warfighter and other agency customers.

- **Agency Contacts** lists the addresses and telephone numbers of agency information offices and key business personnel.

- **Public Info** contains Frequently Asked Questions (FAQs), press releases, speeches, articles, and congressional testimony given by senior agency officials.

- **Library** contains DLA directives, policy letters, fact sheets, biographical information about senior leaders, and other easy-to-read information. To ensure privacy is considered, discretion must be exercised when including biographical information about an individual outside the realm of his or her professional responsibilities and record of achievements.

- **Search** links to a search engine that allows the user to easily conduct a search of agency documents and information systems.

- **Other Sites** lists links to the homepages of the agency's business areas at headquarters and their related field activities, other Defense Department sites, and select academic and business sites. DLA activities' homepages must clearly identify themselves as an entity of the Defense Logistics Agency. Linkages to academic and business sites should be limited to those organizations that have some form of strategic business partnership with DLA activities.

- **Text Only** enables the user to eliminate homepage graphics.

- **Notices** contains information about access and authorization restrictions to government computer systems; such a notice must appear on all DLA homepages. In addition, any DLA page that links to a commercial business partner should contain a **Disclaimer of Endorsement** and, as necessary, **Copyright**- and **Trademark**-protection language. Appendix C provides recommended language regarding each of these subjects.

- **Last Updated** is a notice appearing at the bottom of all homepages that informs the user of the information's currency. Webmasters may wish to consider implementing a regularly scheduled update cycle (e.g., weekly, monthly, or quarterly).

- **Webmaster@[activity's abbreviation].dla.mil** appears at the bottom of the homepage and links the user by e-mail to the technical maintainer of the Web site. The Web site user should be advised that the Webmaster, who is responsible for troubleshooting the site's problems and ensuring that all system elements work properly, is the person to be contacted only about questions or comments on the site's technical issues; comments related to DLA policy and requests for program information should be directed to the site's information or business office, the addresses and telephone numbers of which should be available under **Key Personnel**.

DLA Homepage **CIO Homepage** **Internet Policy Index**

SECURITY

The Internet is an inherently unsecured and constantly expanding series of networks. Information travels across the Internet from origin to destination through unknown and uncontrolled electronic pathways and is vulnerable to interception at any point along the way. Although interception by unauthorized personnel is illegal and subject to criminal prosecution, interceptions will still occur and must therefore be taken into consideration before transmitting or posting potentially sensitive unclassified information—for example, clusters of unclassified information that in aggregate result in conclusory information that is classified or procurement-sensitive.

There are various levels and methods of ensuring information security:

- **Filtering** restricts DLA homepage access to domain addresses ending in ".mil" or "dla.mil," which provides a minimal level of protection for information not cleared for public release.

- A **cul-de-sac** is a server unconnected to any other servers and as such may be used to control access to sensitive agency databases.

- **Firewalls** are specialized computer systems that control entry into a network from remote sites.

- **Passwords** are a means of authenticating a legitimate user's identification.

- **Fortezza cards** are credit card-sized devices that can be inserted into a computer to provide a digital signature, limited encryption, and enhanced identification and authorization capabilities. These cards enable a business concept known as non-repudiation—that is, they create an undeniable electronic record proving that the individual requesting a business transaction initiated and approved the transaction.

A serial combination of access and security controls is required to fully protect information technology systems. All such systems and the networks that connect them to the Internet must employ appropriate security safeguards and must be approved by a Designated Approval Authority.

For more details on network security, see DLA Regulation No. 5200.17, “Security Requirements for Automated Information and Telecommunications Services,” dated 9 June 1993. For further information about the mechanics of establishing network and information technology security, contact Jeffrey Roth of the DLA Systems Design Center (at 614-692-9898, DSN 850-9898, or **jroth@dsdc.dla.mil**) or Timothy Barb of the Office of Command Security at DLA headquarters (at 703-767-5434, DSN 427-5434, or **timothy_barb@hq.dla.mil**).

DLA Homepage **CIO Homepage** **Internet Policy Index**

OVERSIGHT

The Defense Logistics Agency established its **Internet Policy Council** as a mechanism for oversight of the Web sites established by agency field activities and elements of headquarters' operations. Chaired by the CIO's Senior Internet Policy Advisor, it comprises representatives of Acquisition, Materiel Management, Comptroller, General Counsel, the DLA Labor-Management Partnership Council, and Corporate Administration's offices of Public Affairs, Command Security, and Information Services.

The Council is responsible for ensuring compliance with the agency's Internet policy. In that regard, the Council:

- Approves the development, design, and information content of the headquarters' homepage (**http://www.dla.mil**) and its related pages. This process works as follows:

  - Program and project managers seeking approval of a new Web site create a prototype on a disk and present the disk for review by the Council, which in turn reviews the proposed content and page design. The Council also requires the managers to present a short briefing that includes, at a minimum, a discussion of the site's purpose, its targeted audience, and a review of the risk analysis. The Council, which meets on the second Wednesday of each month, typically reviews prototypes within 30 days of the request for review; such requests should be directed to the Senior Internet Policy Advisor, **larry_wilson@hq.dla.mil**, for pre-review and scheduling.

- Assigns and oversees the Webmaster for the headquarters' page and determines the location of its public server.

In addition, the Council periodically reviews all DLA Internet sites to ensure appropriateness of content and appearance and, as necessary, recommends limiting, changing, and removing sites. The members of the headquarters Council strongly recommend the formation of councils at field activities to perform similar oversight functions.

DLA Homepage **CIO Homepage** **Internet Policy Index**

GOVERNMENT INFORMATION LOCATOR SERVICE (GILS)

As part of the U.S. National Information Infrastructure and in compliance with the Paperwork Reduction Act of 1995, the federal government is establishing a **Government Information Locator Service.** A decentralized collection of agency-based information locators and associated information services, GILS identifies publicly available information resources throughout the federal government, describes the information in those resources, and helps individuals and organizations easily locate and access that information, regardless of form or medium.

DLA Web sites representing the business areas at the headquarters and their related primary-level field activities are required to register by submitting records about the sites to the GILS administrator at **http://www.dtic.mil/index/form.html**. Those submitting records are encouraged to read the instructions thoroughly before opening the form. Upon receipt of the GILS record, the administrator will link your site to DefenseLINK.

In the future, the GILS administrator will automatically forward a copy of agency GILS records to DLA's Senior Internet Policy Advisor; however, until that utility is installed, DLA activities submitting records are asked to provide a copy to **larry_wilson@hq.dla.mil** or by fax to the advisor at 703-767-3153. Note that GILS records must be updated every six months.

DLA Homepage **CIO Homepage** **Internet Policy Index**

APPENDIX A:
LAWS AND REGULATIONS

In complying with legal and regulatory requirements, the following may be pertinent to the collection, dissemination, accession, and preservation of government information resources.

- **Freedom of Information Act** (5 U.S.C. 552).

- **Privacy Act** (5 U.S.C. 552a, OMB Circular A-130).

- **The Paperwork Reduction Act** (44 U.S.C. Chapter 35, amended in 1995).
  See text at **http://www.whitehouse.gov/WH/EOP/OMB/html/circulars/a130/a130.html**.

- **The Information Technology Management Reform Act of 1996** (Public Law 104-106, Sec. 5001).

  Chief Financial Officers Act (31 U.S.C. 3512 et seq).

- **Federal Property and Administrative Services Act** (40 U.S.C. Sec. 759 and Sec. 487).

- **Federal Records Act** (44 U..S.C. Chapters 29, 31, 33, 35), **National Archives and Records Administration Regulations** (36 CFR Chapter 12, Subchapter B, "Records Management").

- **Computer Security Act** (40 U.S.C. 759 note).
  See text at **http://www.net.ohio-state.edu/hypertext/csa-1987.html**.

- **Budget and Accounting Act, as amended** (31 U.S.C. Chapter 11).

- **Management of Federal Information Resources** (OMB Circular A-130 (Revised)).

- **Establishment of Government Information Locator Service** (OMB Bulletin No. 95-01).

- **Clearance of DoD Information for Public Release** (DoD Directive 5230.9, 9 April 1996).
  See text at **http://www.dtic.mil/adm/data/5230.html**.

- **Joint Ethics Regulation** (DoD Regulation 5500.7, 30 August 1993, amended 25 March 1996).

- **Security Requirements for Automated Information and Telecommunications Systems** (DLA Regulation No. 5200.17, 9 June 1993).

- **Use of DoD Information and Telecommunications Systems** (Memorandum from the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, 1 February 1997).

- **Clearance Procedures for Making Electronic Information Available to the Public** (Memorandum from the Deputy Secretary of Defense, 17 February 1995).

- **Instructions for Submitting Government Information Locator Service Records** (Memorandum from the Office of the Secretary of Defense, 5 December 1995).

- **Guidelines for Establishing and Maintaining a Department of Defense Web Information Service** (draft memorandum from the Assistant Secretary of Defense for Public Affairs, 12 March 1997).

DLA Homepage **CIO Homepage** **Internet Policy Index**

APPENDIX B:
DEFINITIONS

The following are common terms, acronyms, abbreviations, and definitions in the world of the Internet.

CIO **Chief Information Officer**: The Information Technology Management Reform Act of 1996 mandates that Executive Branch agencies designate a CIO in order to establish clear accountability for agency Information Resource Management programs and investments, to provide greater coordination among an agency's information activities, and to monitor and evaluate the performance of Information Technology initiatives. The law also states that the CIO must report to the agency's head and hold the rank of other senior-level officials.

Content Providers These are the business-area experts who develop the technical and functionally related information that comprises the Web's content and who advise the Public Affairs Officer on its releasability.

e-mail This is the abbreviation for electronic mail.

FAQ **Frequently Asked Questions**

Firewall This is a term for software that limits user access to a network.

FOIA **Freedom of Information Act**

FOUO **For Official Use Only**: This designation indicates that information, while not technically classified, is to be used only by authorized government and contractor personnel and is not intended for dissemination to the general public.

FTP **File Transfer Protocol**: This is the means by which files are transferred between systems on the Internet.

GILS **Government Information Locator Service**: Extensive information about this cataloged repository of publicly released documents can be found at **http://www.dtic.mil/index** or **http://www.usgs.gov/gils/index.html**.

Homepage This is the page of visual imagery and textual information that initially appears on the computer monitor of a user accessing an Internet address. DLA homepages are intended to greet the user, identify the activity and its mission, and quickly guide the user to desired information about the activity's programs and services.
HTTP **HyperText Transfer Protocol**: This defines how documents published on the Internet are formatted, displayed, and linked to other documents.

INFOSEC **Information Security**

ISDN **Integrated Services Digital Network**

Internet This is an informal collection of government, military, commercial, and educational computer networks used to transmit information electronically. This worldwide group of networks uses gateways to convert files to standard formats and protocols. Maintained by a private-sector Internet Architecture Board, the "Net" uses protocols built on the TCP/IP transport.

Intranet This is a technological clone of the Internet, but access is restricted to an organization's internal audience—and by invitation, selected business partners.

LAN **Local Area Network**: This indicates the technologies used to connect a number of personal computers in a limited area such as a single building or section thereof.

NIC **Network Interface Card**

PPP **Point-to-Point Protocol**: This allows point-to-point links, such as modem-to-modem connections, to communicate and transport higher-layer protocols such as TCP/IP.

SLIP **Serial Link Internet Protocol**: This allows TCP/IP traffic to travel across a serial link such as a modem.

TCP/IP **Transport Control Protocol/Internet Protocol**: This is the *language* used by systems on the Internet to communicate.

WAN **Wide Area Network**: This name indicates the technologies used to connect multiple personal computers, mainframes and file servers over a geographically dispersed area using long-distance communications.

WWW **World Wide Web**: The “Web,” as it is often called, is a collection of protocols and standards that allow users to quickly and easily find and distribute information over the Internet. Its core language or protocol is hypertext markup language, or HTML.

DLA Homepage **CIO Homepage** **Internet Policy Index**

APPENDIX C:
NOTICES

The following is recommended language regarding notice, disclaimer, copyright, and trademark links, the latter three to be used as necessary:

Notice. This World Wide Web site is provided as a public service of the Defense Logistics Agency. It allows the public to view and retrieve information only. By accessing this site, you are consenting to system monitoring for law enforcement and other purposes. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986. All information on these pages is considered public information and may be distributed and copied.

Disclaimer of Endorsement. Reference on this World Wide Web site to a specific contractor or commercial product, process, or service does not constitute or imply an endorsement or recommendation by the Defense Logistics Agency.

Copyright or **Trademark Status**. This document is protected under copyright/trademark law. Permission to reproduce or use the document must be obtained from the copyright/trademark holder.

DLA Homepage **CIO Homepage** **Internet Policy Index**